(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
2 December 2004 (02.12.2004)

PCT

(10) International Publication Number
WO 2004/105340 A1

(51) International Patent Classification[7]: H04L 29/06

(21) International Application Number:
PCT/EP2004/050889

(22) International Filing Date: 21 May 2004 (21.05.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0311921.1 23 May 2003 (23.05.2003) GB

(71) Applicant *(for all designated States except US)*: TELEFONAKTIEBOLAGET LM ERICSSON (publ) [SE/SE]; S-16483 Stockholm (SE).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: NIKANDER, Pekka [FI/FI]; OY LM Ericsson AB, FIN-02420 Jorvas (FI). ARKKO, Jari [FI/FI]; Kauppalantie 25 A 7, FIN-02700 Kauniainen (FI).

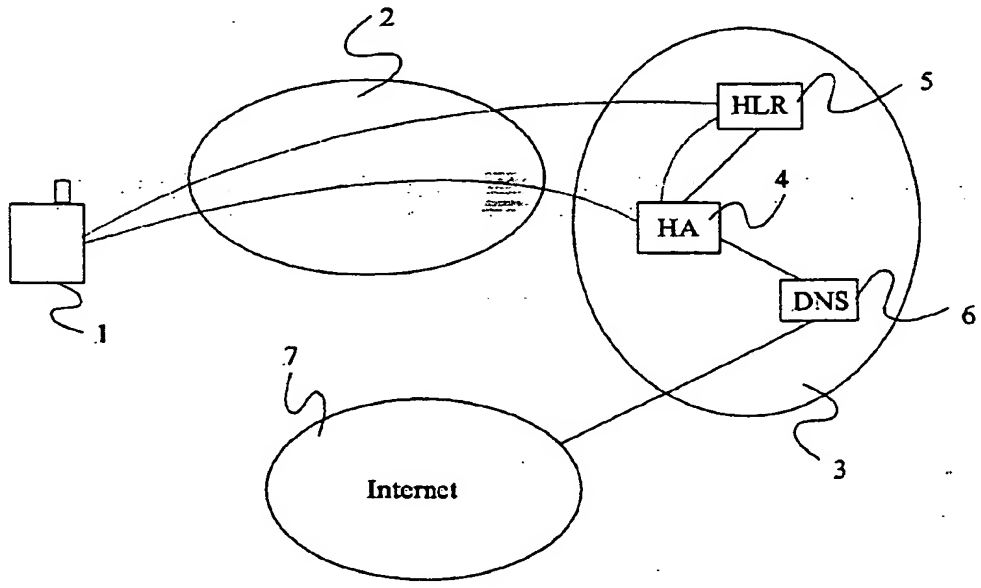
(74) Agents: LIND, Robert et al.; 4220 Nash Court, Oxford Business Park South, Oxford Oxfordshire OX4 2RU (GB).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: SECURE TRAFFIC REDIRECTION IN A MOBILE COMMUNICATION SYSTEM



(57) Abstract: A method of securely initialising subscriber and security data in a mobile routing system when the subscribers are also subscribers of a radio communication network. The method comprises, within the mobile routing system, authenticating subscribers to the mobile routing system using an authentication procedure defined for the radio communication network, collecting subscriber information from relevant nodes of the radio network, and agreeing upon keys by which further communications between the subscribers and the mobile routing system can take place, and using said subscriber information and keys in the provision of mobility services to subscriber mobile nodes and correspondent nodes.

WO 2004/105340 A1

Published:

— *with international search report*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Secure Traffic Redirection in a Mobile Communication System

Field of the Invention

The present invention relates to secure traffic redirection in a mobile communication system and in particular to a method and apparatus for enabling a mobile node to securely perform transactions, relating to traffic redirection, with a home network.

Background to the Invention

In traditional cellular telephone networks, mobile nodes are able to roam between cells without the need to drop ongoing telephone calls. With the introduction of mobile IP services, solutions have been sought to allow mobile IP nodes to roam within and even between different access networks (such as UMTS or WLAN) with only the minimum disruption to services. The preferred solutions are based on the idea of allowing traffic flows to be redirected to the current location of the mobile node.

In one solution, known as Mobile IPv6, the traffic flows are identified by a stable IPv6 address and are routed to the home network of the mobile node before forwarding to the current "care-of-address" of the mobile node. When the mobile node roams between access nodes, an update message containing a new care-of-address is sent to the home network. In another solution known as Host Identity Protocol (HIP), a public key (or a hash of a public key) identifies the traffic flows. In either case, a stable forwarding agent is required somewhere in the network so that other nodes can contact the mobile node without previous knowledge of the current location of the mobile node.

In Mobile IPv6, this stable forwarding agent is called the Home Agent, and a security association must exist between the Home Agent and the mobile node in order to prevent unauthorised location updates being acted upon. In HIP, there is no need for such a security association as the public key can be used directly to identify a particular node in a secure manner. However, in order for other nodes to learn the public key of the HIP-based mobile node, this public key must be stored in a Domain Name System (DNS) server in a secure manner. Therefore, in both cases the mobile node must be capable of securely performing transactions with its "home network", either for the

purpose of talking to its Home Agent or for updating the DNS server to store its public key at the deployment phase.

Typically, the set-up of the security association (SA) for the home agent or the update of the DNS server might be performed manually. While parts of these operations have been automated, for instance through the use of a public key infrastructure, the authorisation step has to date remained a manual operation. In Mobile IPv6, this step involves a decision on whether the particular mobile node (even with a certificate from a trusted third party) is allowed to use a particular IPv6 address. This step is not easy to automate through public key infrastructure, given that the infrastructure would typically be unable to tell which IP address assignments are made in the network. In HIP, the procedure is easier but requires the existence of a public key infrastructure and requires that a determination has been made as to whether the mobile node is allowed to control the given domain name. The existence of such a public key infrastructure can be seen as redundant and unnecessary, given that the purpose of the DNS system is to act as a public key infrastructure – it would be strange to require another public key infrastructure to enter data into a DNS server.

The above technical problems are likely to lead to a service deployment problem in future networks. It is unacceptable from a business perspective to require manual work in order to set up each and every mobile node (out of millions) for the mobility service.

Summary of the Invention

It is an object of the present invention to make use of existing security mechanisms to bootstrap whatever security may be required by the mobility services and mechanisms.

According to a first aspect of the present invention there is provided a method of securely initialising subscriber and security data in a mobile routing system when the subscribers are also subscribers of a radio communication network, the method comprising:

within the mobile routing system, authenticating subscribers to the mobile routing system using an authentication procedure defined for the radio communication network, collecting subscriber information from relevant nodes of the radio network,

and agreeing upon keys by which further communications between the subscribers and the mobile routing system can take place; and

using said subscriber information and keys in the provision of mobility services to subscriber mobile nodes and correspondent nodes.

Preferably, messages associated with said step of authenticating subscribers to the mobile routing system are transported between the mobile node used by a subscriber and an authentication server of the subscriber's home network via a mobility server. The mobility server collects subscriber information from relevant nodes (subscriber databases) of the cellular radio network, and receives a shared key or key from the authentication server following completion of the re-run authentication procedure.

Preferably, session keys agreed upon during the re-run authentication procedure are sent by the authentication server to the mobility server.

In a first embodiment of the invention the mobile routing system is a MobileIP based system, in which case the mobility server is a Home Agent. In an alternative embodiment of the invention the mobile routing system is a HIP based system and the mobility server is a Forwarding Agent.

By way of example, said authentication procedure may be the Authentication and Key Agreement (AKA) procedure. Other procedures may of course be utilised.

According to a second aspect of the invention there is provided a method of operating a mobile node for use in a mobile radio communication system, the method comprising:

initiating an authentication procedure defined for the radio communication network, for the purpose of authenticating the mobile node to a mobile routing system, and conducting said procedure with an authentication server via a mobility server of the mobile routing system.

According to a third aspect of the present invention there is provided a method of operating a mobility server of a mobile routing system, the method comprising:

relaying messages associated with an authentication procedure, between a mobile node and an authentication node;

following completion of said procedure, receiving a shared secret from the authentication server, and collecting subscriber information from the authentication server and/or other network nodes; and

using said subscriber information and keys in the provision of mobility services to subscriber mobile nodes.

According to a fourth aspect of the present invention there is provided a method of operating an authentication server of a mobile radio communication network, the method comprising;

conducting an authentication procedure with a mobile node via a mobility server; and

sending a shared secret resulting from said procedure to said mobility server.

Brief Description of the Drawings

Figure 1 illustrates schematically a mobile radio communication system incorporating a mobility routing system.

Detailed Description of Certain Embodiments

Procedures have been defined and specified for allowing a mobile node to be securely authenticated by a home network in a cellular communication system. For example, the 3GPP authentication procedure known as Authentication and Key Agreement (AKA) makes use of a secret key stored in the Subscriber Identity Module (SIM) card of a cellular device and in the HSS node of the subscriber's home network to authenticate the cellular device (or rather the SIM card) at the network level. In the case of a roaming cellular device, the AKA procedure is performed via the visited network, with the home network informing the visited network of the authentication decision. Whilst alternatives to AKA exist and fall within the scope of this invention, the present discussion will be restricted to AKA by way of example.

Use of the AKA procedure for network level authentication will typically allow a subscriber to make phone calls but does not necessarily authenticate a mobile node for

particular services. Considering IP mobility services such as Mobile IP and HIP, a separate authentication procedure is required. As already discussed, these separate procedures have in the past been carried out manually.

It is proposed here to reuse the AKA procedure and the associated secret shared between a mobile node (SIM card) and a home network for the purpose of authenticating a mobile node to a mobile routing system. Considering firstly the case of Mobile IP, Figure 1 illustrates in simplified form a typical system architecture. A mobile node 1 is currently attached to a visited network 2. It is assumed that the AKA procedure has previously been run in order to authenticate the mobile node to the home network 3 and hence to the visited network 2. The mobile node 1 therefore has access to the foreign network at the network level. The procedure may comprise the following steps:

Step 1. The mobile node 1 establishes (IP) network connectivity by establishing a connection through GPRS, for instance. As already stated, this step assumes that the AKA procedure has been carried out to provide network access authentication. However, this step is considered to be independent from the IP mobility authentication procedure, even if both procedures use the same SIM card.

Step 2. The mobile node initiates an authentication procedure with the Home Agent 4 of the mobile routing system.

Step 3. The Home Agent 4 relays messages between the mobile node 1 and the authentication server (HLR) 5 of the home network 3 in order to execute (i.e. re-run) the AKA (USIM) authentication between the Home Agent and the mobile node. This involves the following steps:

- The mobile node 1 sends its identity to the HLR.
- The HLR 5 sends a challenge to the mobile node 1.
- The mobile node 1 optionally verifies the authenticity of the HLR's challenge.
- The mobile node sends a response to the HLR.
- The HLR verifies the authenticity of the mobile node's response.
- The HLR optionally sends an acknowledgement back to the mobile node.

- Both the mobile node and the HLR establish shared session key(s), such as the USIM CK and IK.

Step 4. The HLR 5 forwards the results of the re-run AKA procedure (including session keys) to the Home Agent 4.

Step 5. The mobile node 1 generates a public key pair.

Step 6. The mobile node 1 sends a message to the Home Agent 4, protected using the shared session key(s) established in Step 3. The message contains the following information:

- The public key of the mobile node.
- An optional signature of the mobile node, made using the private key associated with the public key.
- Optional desired parameters, such as a desired fully qualified domain name (FQDN).
- Optional shared secret (if provided, this part must be encrypted).

Step 7. The Home Agent 4 verifies the authenticity of the mobile node's message through the use of the shared session key(s) and optionally using the signature.

Step 8. The Home Agent 4 collects certain predefined information from the HLR 5 and possibly other subscriber databases, as well as the current contents of the local DNS server 6 (zone). This information may comprise for example:

- The name and postal address of the user associated with this SIM card.
- The telephone number associated with this SIM card.
- The existing FQDNs in the DNS (either for this particular subscriber or for others).
- The status of any mobility services established earlier for the particular subscriber or SIM card.

Step 9. The Home Agent 4 makes a decision about a suitable FQDN and/or IP address which can be assigned to the device. For instance, the Home Agent can check the desired FQDN for consistency with the operator's domain name (e.g. sonera.net), the user's phone number or name (e.g., matti-virtanen.sonera.net), and the existence of

possible previous entities with the same FQDN. The Home Agent also makes the necessary configurations in the following entities:

The local DNS server 6 (using for example the Dynamic DNS protocol), where the selected FQDN and the associated public key are stored.

- One or more of the subscriber databases (possibly including a change in the billing information).

Step 10. The Home Agent 4 communicates the configuration back to the mobile node, including:

- The chosen FQDN and, optionally, IP address
- Optionally, the public key of some network node used by the device (such as the Home Agent).

Step 11. The mobile node 1 stores the received information. Note that this information has to be handled in a special way if a separation exists between a device and the user's credentials such as is common in phones and SIM cards inserted into them. Leaving the information in the device for use by any user (SIM card) would allow the use of this information by other users. This risk can be mitigated by storing the received information in the SIM, or storing it in the device in a manner which isn't accessible after another SIM has been inserted.

As a result of the AKA re-run and the collection and distribution of data by the Home Agent, the mobile node can now use mobility services in a secure manner. Communications between the Home Agent and the mobile node can be secured using the public key and/or shared secret.

Considering the HIP scenario, the Home Agent is replaced by a Forwarding Agent (or anchor point). It is the Forwarding Agent which acts as the intermediary between the mobile node and the HLR during the AKA re-run. In addition to the procedures outlined above, in Step 9 the address of the Forwarding Agent is stored in the DNS server. The mobile node's public key and the address of the forwarding agent can then be retrieved by third parties from the DNS server via the Internet 7, and communications can flow to the mobile node regardless of its current position and IP address.

There exists proposals that make use of cell phone authentication in other contexts (e.g. RFC 3310), so the reuse of SIM authentication itself is not new. Here, however, the authentication procedure in a specific way for a specific application, with additional procedures for collecting at the mobility server (i.e. the Home or Forwarding Agent) information from the subscriber database or databases.

There exists proposals that make use of cell phone authentication even in the context of, e.g., Mobile Ipv6. However, these proposals use such authentication each time a transaction is carried out between the mobile node and the mobility server, and lack a mechanism to decide the IP addresses and FQDNs.

There also exists proposals to use cell phone and other legacy authentication mechanisms to generate so called subscriber certificates in a general fashion, suitable for any application. However, the solutions described here avoid this step, and avoid the use of any PKI other than the resulting DNS system as a "weak" form of PKI. In addition, the presented solutions are clearly able to make the necessary authorisation decisions regarding FQDNs and IP addresses, unlike the existing proposals

Standard protocols exist for making dynamic updates to DNS. However, currently these are secured with pre-provisioned shared secrets (DNS TSIG) or other mechanisms which can provide a shared secret, such as Kerberos (GSS TSIG) or secure DNS. All of these mechanisms today make the security decisions without regard to the specific entity that is making the request. This is insufficient, as it is necessary for a specific node to control its own IP address and DNS name, but not the addresses and names of other nodes. The proposals presented here deal with this by combining the user database and the authentication procedure.

Embodiments of the invention should enable easy deployment of mobility services in heterogeneous networks.

The above discussion has considered the scenario where the access network is the same when both the initial, network level authentication procedure and the re-run procedure are carried out. A question to be addressed is what happens if a mobile node moves

between different access networks which might use different authentication procedures. Consider for example the scenario in which a mobile node roams between a UMTS access network and a WLAN access network. Whilst the UMTS network will use AKA to authenticate subscribers at the network level, the WLAN network might use some other procedure at this level. The present invention encompasses the possibility that, after the WLAN network level access procedure has been carried out, the AKA procedure is reused to authorise the subscriber in respect of the mobility service.

It will be appreciated by the person of skill in the art that various modifications may be made to the embodiments described above without departing from the scope of the present invention.

Claims:

1. A method of securely initialising subscriber and security data in a mobile routing system when the subscribers are also subscribers of a radio communication network, the method comprising:

within the mobile routing system, authenticating subscribers to the mobile routing system using an authentication procedure defined for the radio communication network, collecting subscriber information from relevant nodes of the radio network, and agreeing upon keys by which further communications between the subscribers and the mobile routing system can take place; and

using said subscriber information and keys in the provision of mobility services to subscriber mobile nodes and correspondent nodes.

2. A method according to claim 1 and comprising transporting messages associated with said step of authenticating subscribers to the mobile routing system, between the mobile node used by a subscriber and an authentication server of the subscriber's home network, via a mobility server.

3. A method according to claim 2 and comprising collecting subscriber information from relevant nodes of the mobile network at the mobility server, and receiving a shared secret or secrets from the authentication server following completion of the re-run authentication procedure.

4. A method according to claim 3 and comprising sending session keys, agreed upon during the re-run authentication procedure, from the authentication server to the mobility server.

5. A method according to any one of claims 2 to 4, wherein the mobile routing system is a MobileIP based system, and the mobility server is a Home Agent.

6. A method according to any one of claims 2 to 4, wherein the mobile routing system is a HIP based system and the mobility server is a Forwarding Agent.

7. A method according to any one of the preceding claims, wherein said authentication procedure is the Authentication and Key Agreement procedure.

8. A method according to any one of the preceding claims, wherein the collected subscriber information comprises one or more of the following:

the name and postal address of the subscriber;

the telephone number associated with the subscriber;

the existing Fully Qualified Domain Name for the subscriber; and

the status of any mobility services established earlier for the subscriber.

9. A method of operating a mobile node for use in a mobile radio communication system, the method comprising:

initiating an authentication procedure defined for the radio communication network, for the purpose of authenticating the mobile node to a mobile routing system, and conducting said procedure with an authentication server via a mobility server of the mobile routing system.

10. A method of operating a mobility server of a mobile routing system, the method comprising:

relaying messages associated with an authentication procedure, between a mobile node and an authentication node;

following completion of said procedure, receiving a shared secret from the authentication server, and collecting subscriber information from the authentication server and/or other network nodes; and

using said subscriber information and keys in the provision of mobility services to subscriber mobile nodes.

11. A method of operating an authentication server of a mobile radio communication network, the method comprising;

conducting an authentication procedure with a mobile node via a mobility server; and

sending a shared secret resulting from said procedure to said mobility server.

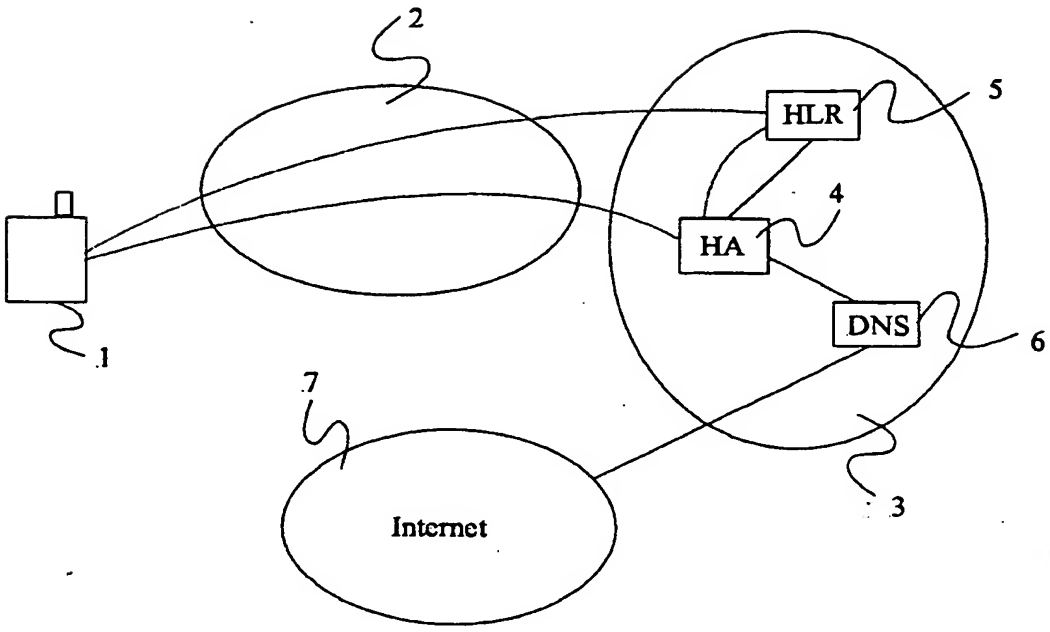


Figure 1